Deloitte. Insights

A report from the
Deloitte Center for Financial Services

Overcoming challenges to cyber insurance growth

Expanding stand-alone policy adoption among middle market businesses

About the Deloitte Center for Financial Services

The Deloitte Center for Financial Services (DCFS), which supports the organization's US Financial Services practice, provides insight and research to assist senior-level decision-makers within banks, capital markets firms, investment managers, insurance carriers, and real estate organizations. The center is staffed by a group of professionals with a wide array of in-depth industry experiences as well as cutting-edge research and analytical skills. Through our research, roundtables, and other forms of engagement, we seek to be a trusted source for relevant, timely, and reliable insights. Read recent publications and learn more about the center on Deloitte.com. For weekly actionable insights on key issues for the financial services industry, check out the Deloitte Center for Financial Services' Quicklook articles.

Connect

To learn more about the vision of the DCFS, its solutions, thought leadership, and events, please visit www.deloitte.com/us/cfs.

Subscribe

To receive email communications, please register at www.deloitte.com/us/cfs.

Engage

Follow us on Twitter at @DeloitteFinSvcs.

Contents

KEY MESSAGES

Dear colleagues,

Insurance company leaders, like those at most organizations, are grappling with unprecedented challenges brought on by the COVID-19 outbreak—taking care of clients, employees, and distributors while maintaining business continuity. At the same time, many will still likely have to deal with a number of market challenges that arose well before the outbreak. One such issue was how insurers might bolster sales of stand-alone cyber insurance policies, which have been well below the industry's initial expectations despite the rise in cyber-related events. We surveyed cyber insurance buyers and brokers in the summer of 2019 to learn more. Among our main findings:

- Despite the increasing frequency and severity of cyberattacks, US sales of dedicated cyber insurance policies remain relatively low and growth is far below industry expectations. Cyber insurance overall only generates around US$2 billion in annual premiums, with 42 percent coming from more limited coverage included in standard multiperil policies.
- Concerns about cost and coverage limits were the top two reasons cited by middle market insurance buyers surveyed for not taking a stand-alone cyber policy. Many passed because they already had some cyber coverage included in standard commercial policies.
- Many agents and brokers charged with selling stand-alone cyber policies do not appear to be pushing the product aggressively. In fact, some are dissuading customers from buying the coverage, citing concerns about its value and claims payment issues.
- Fear is a big factor spurring cyber insurance sales. Middle market respondents who had endured a cyber loss or had heard about attacks against others in their industry or supply chain were much more likely to buy a stand-alone policy. Nonbuyers were more likely not to have experienced an attack.
- To drive faster stand-alone policy growth, insurers will likely have to rethink pricing strategies, offer cyber risk management services and corresponding premium incentives, and invest more in educating both buyers and brokers about cyber risk and the advantages of dedicated coverage.

Despite rising risk, cyber insurers struggle to gain traction

IT SEEMS HARDLY a day goes by without a report of a new cyberattack. Sixty-one percent of companies surveyed worldwide by Hiscox reported one or more events in 2019, up from 45 percent a year earlier, with both frequency and severity rising considerably.[1] And while the headlines usually feature hackers targeting the largest companies, 63 percent of midsized firms recorded an event last year, up substantially from 2018's total of 36 percent.[2] The mean cost of an event for midsized companies more than quadrupled, from US$44,000 to US$184,000, in part due to increasingly frequent ransomware attacks.[3]

Given such a risky environment, you might expect the market for a dedicated, stand-alone cyber insurance policy to be expanding exponentially. Yet the industry still has a long way to go to fulfill such lofty expectations.

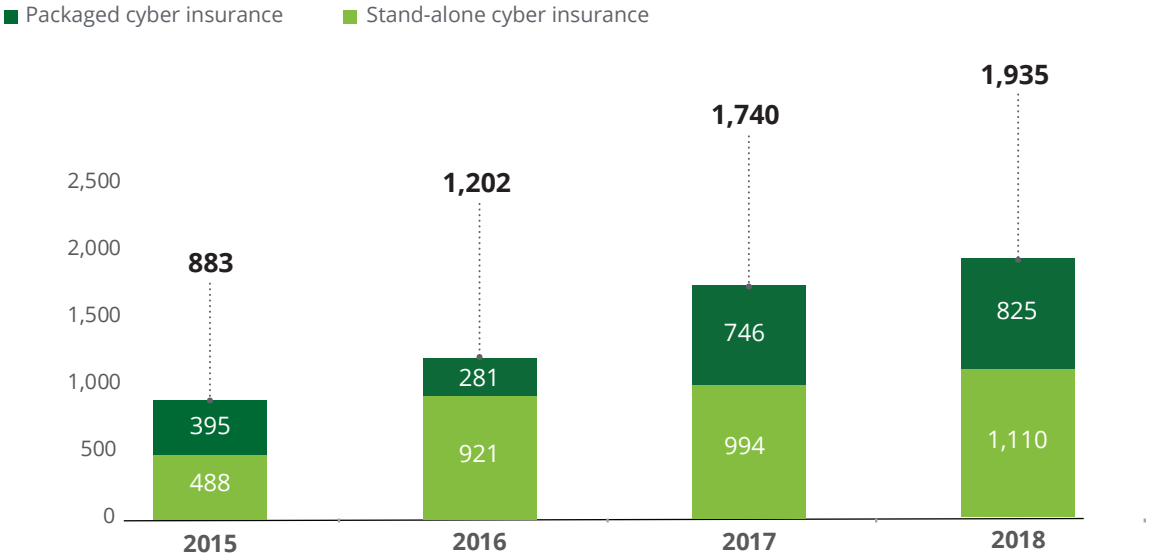
Not too long ago, some in the industry, such as Allianz, predicted that cyber premiums could reach US$20 billion or more by 2025.[4] In fact, net written premiums in the United States totaled only US$1.94 billion in 2018—with 58 percent (US$1.12 billion) generated by stand-alone policies and the remaining 42 percent by cyber coverage included in standard commercial policies (figure 1).[5] While cyber premiums from standard policies jumped dramatically between 2016 and 2017 (figure 2), that could partly be due to adjustments in reporting after US insurance regulators began requiring insurers to approximate what they collected or allocated specifically for cyber risks.[6]

Given these lower-than-expected results, some market leaders seem less optimistic about the future of cyber insurance. Aon noted that "markedly reduced growth in 2018 gives pause and causes us to question whether the cyber insurance industry can live up to the aggressive growth projections that have been made."[7]

FIGURE 1

US cyber insurance premium growth slowing

Cyber insurance direct premiums written (US$ millions)

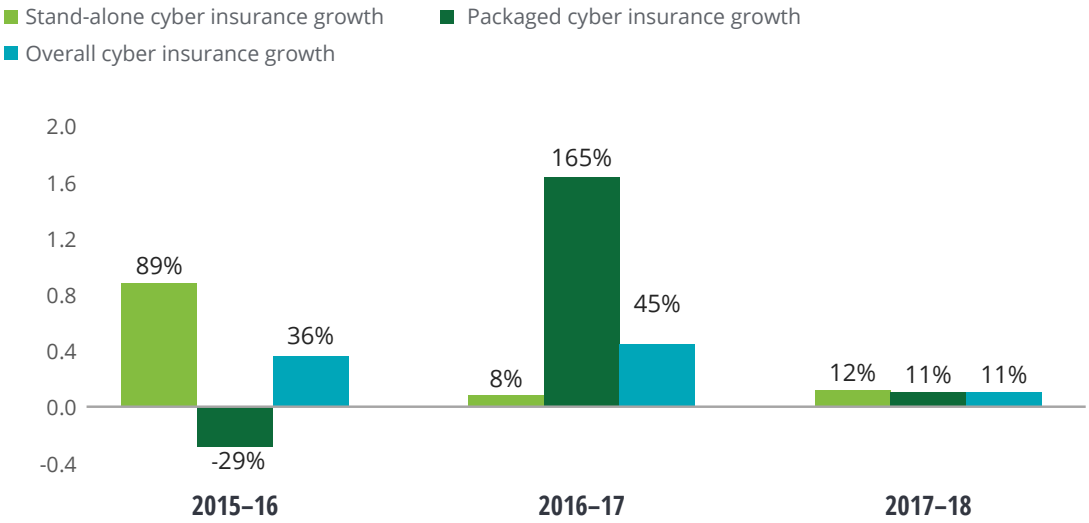


Source: Data from S&P Global Market Intelligence; Deloitte Center for Financial Services analysis.

FIGURE 2

Stand-alone cyber policy premium growth remains modest

Cyber insurance direct premiums written year-over-year growth (percent)



Source: Data from S&P Global Market Intelligence; Deloitte Center for Financial Services analysis.

Many insurers are looking to sell stand-alone cyber insurance to supplement, if not replace, coverage bundled in standard policies, which were likely not designed to protect against today's fast-moving cyber risk landscape. Over the years, the industry took similar steps to spin off other challenging specialty lines, such as directors and officers (D&O) and employment practices liability insurance (EPLI), where the increasing frequency and severity of events made such exposures difficult to address in a generic, multiperil policy. In addition, higher limits would likely be easier to come by in a stand-alone cyber policy, as would reinsurance support to generate greater capacity if the exposure were cordoned off from standard property and liability risks.

Yet, despite the apparent logic of buying stand-alone cyber coverage, there is some cause for concern about the line's future growth prospects. Market penetration remains relatively low, especially for such a high-profile exposure. Fifty-nine percent of companies surveyed by Hiscox do not have any cyber insurance. While 30 percent said they plan to purchase coverage in the next year, nearly as many (26 percent) say they have no such intention.[8] A survey by Marsh found that 43 percent of companies with more than US$1 billion in revenue did not have a stand-alone cyber insurance policy, with the uninsured total soaring to 64 percent for midsized and smaller firms.[9]

Why does there seem to be such widespread reluctance to buy cyber insurance in general, and stand-alone coverage in particular among middle market companies (defined for this report as those with US$250 million to US$1 billion in annual revenue)? Given the amount of press coverage cyberattacks have received, awareness of the exposure should not be lacking. Hiscox found that only 3 percent of buyers surveyed were "unsure what cyber insurance is."[10] Cyber risk is also front and center as a key exposure for management and boards to address, given all the new cybersecurity, privacy, and data use regulations put in place.

To help resolve this conundrum, the Deloitte Center for Financial Services surveyed 504 middle market commercial insurance buyers from five industries (see sidebar, "Methodology"). We also surveyed 103 agents and brokers to gain the seller's point of view.

Our immediate goal was to determine the reasons behind the slower-than-expected adoption rate for stand-alone cyber insurance in the middle market. Such buyers may not be household names, but often have large operations, usually with a full-time risk manager handling insurance purchasing. Among the topics we examined:

- For respondents who passed on stand-alone cyber policies ("nonbuyers"), why did they do so, and what circumstances, if any, might convert them into buyers?
- What factors prompted respondents who bought stand-alone policies ("buyers") to make the purchase? How do they feel about the coverage, and what has been their experience with claims?
- How do buyers and nonbuyers assess the performance of their agents and brokers in helping them deal with cyber risks and insurance to cover such exposures? And what do intermediaries say about their clients' preferences and concerns—as well as their own hesitation in recommending the coverage?

Ultimately, our purpose is to help cyber insurers learn how they might overcome obstacles that are hindering more robust, profitable growth—not just in the middle market, but across the board, commensurate with an expanding exposure.

METHODOLOGY

The Deloitte Center for Financial Services surveyed executives responsible for purchasing insurance at 504 middle market companies, defined as having more than US$250 million but less than US$1 billion in annual revenue. The survey, fielded during the summer of 2019, was not random. Preset quotas required close to a 50-50 split between buyers and nonbuyers of stand-alone policies, regardless of whether they had any cyber coverage in standard policies (figure 3). There were also target levels for five industries included in the study (figure 4).

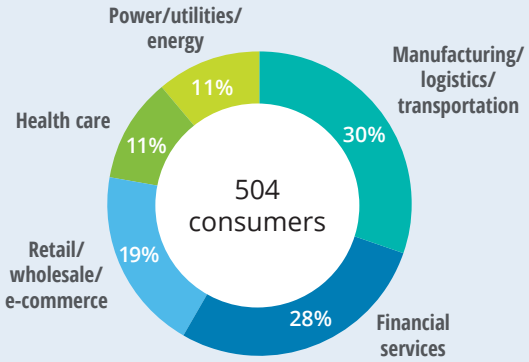
While respondents in the smallest of the three revenue subsets (those with companies generating more than US$250 million but less than US$500 million annually) were the least likely to have stand-alone policies, the upper two subsets still had significant percentages without dedicated coverage.

We also surveyed 103 agents and brokers marketing cyber insurance and serving middle market buyers in two or more of the five target industries (figure 5).

FIGURE 4

Which insurance buyers were surveyed?

Respondent profile, by industry

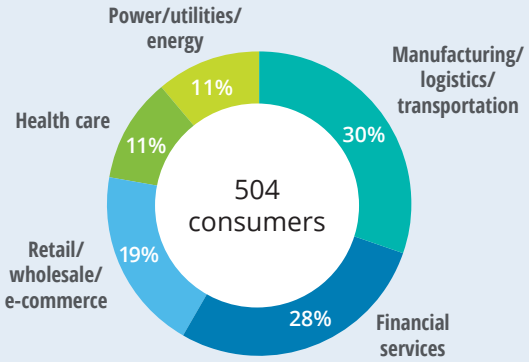


Source: Deloitte 2019 Middle Market Cyber Insurance Survey.

FIGURE 4

Which insurance buyers were surveyed?

Respondent profile, by industry

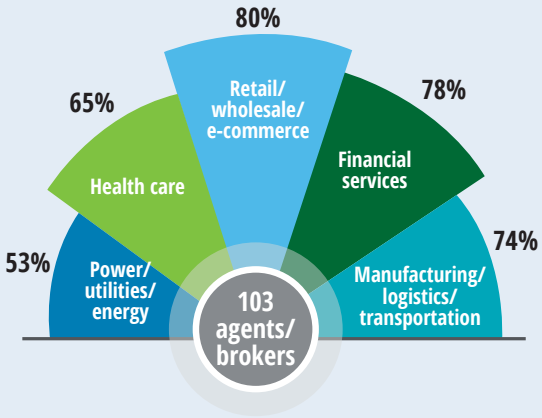


Source: Deloitte 2019 Middle Market Cyber Insurance Survey.

FIGURE 5

Which insurance agents/brokers were surveyed?

Agent/broker respondent profile (percentage of sample serving each target industry)



Source: Deloitte 2019 Middle Market Cyber Insurance Survey.

What has prompted middle market companies to pass on stand-alone coverage?

WE ASKED NONBUYER respondents to list all the reasons they didn't have a stand-alone cyber policy (figure 6) as well as to rank their top three reasons among those chosen.

Cost of coverage was the top reason surveyed health care and financial services buyers cited, and second in the other three industries examined. Yet while cyber insurance premiums have been on the rise of late—up nearly 3 percent in the United States during the third quarter of 2019—that's well below the average 8 percent boost in overall commercial insurance pricing for the quarter.[11] Therefore, rather than shying away because of price hikes, many prospects may be put off by the lack of value they perceive in stand-alone policies. Indeed, "coverage limits too low" was cited by 34 percent of all respondents without any cyber coverage, while 29 percent said coverage terms and exclusions were too restrictive.

Another possible explanation is a lack of budget for what would amount to an additional insurance policy purchase. One risk manager respondent from a manufacturing company wrote that "we didn't have much to cover [stand-alone] in our [insurance] budget," a point that was also raised by buyers speaking at Advisen's 2019 Cyber Risk Insights Conference.

Many prospective buyers may still regard stand-alone cyber coverage as a luxury rather than a necessity. It might represent an unexpected cost that would either have to be squeezed into an already tight budget or require additional funds to accommodate. That may be difficult for some buyers to justify to their C-suite, especially if the limits or terms do not seem attractive enough to make the extra policy worthwhile.

Our survey revealed another major hurdle that insurers face: The reason many companies do not have stand-alone coverage (cited by 43 percent of all nonbuyer respondents) is because they already had cyber risks packaged into their standard property and liability policies. This was the top reason cited by respondents in retail/wholesale/e-commerce, while coming in second among financial services respondents. Agents and brokers surveyed also rated this the number one obstacle to selling stand-alone coverage.

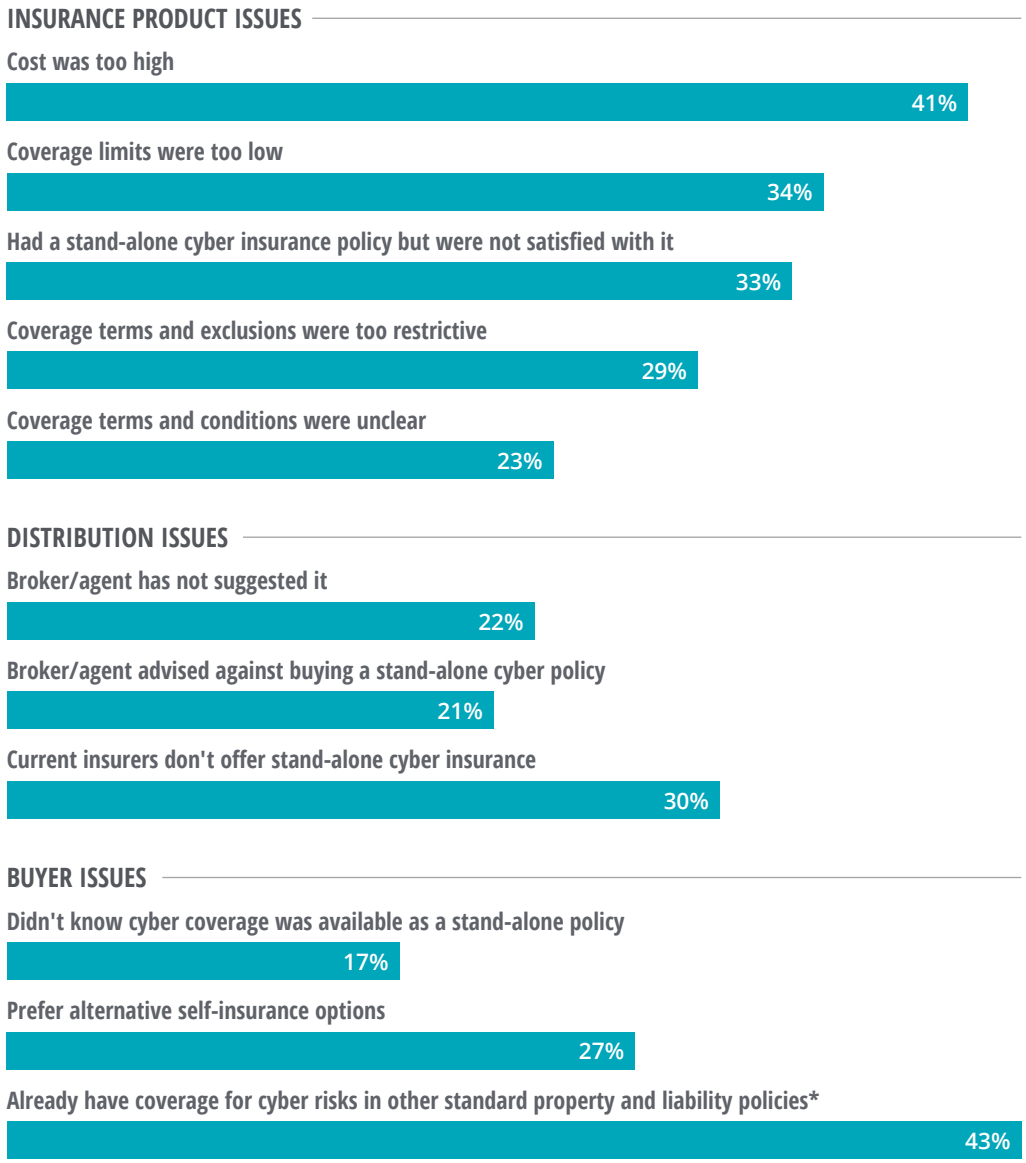
Insurers and their intermediaries, therefore, face a major educational challenge to convince policyholders they need stand-alone coverage, at least to supplement, if not substitute, for any cyber coverage they may have in standard policies. As with directors and officers, employment practices, product liability, and other specialty coverages that are usually sold separately today, stand-alone cyber policies can offer clearer coverage terms and conditions as well as higher, dedicated limits than would be the case with bundling cyber with standard property and liability exposures, such as fire, physical damage, and crime losses.

Purchasing stand-alone could also avoid potential claims disputes over "silent" coverage in a standard

FIGURE 6

Multiple factors kept respondents from buying stand-alone policies

Q: Why hasn't your company purchased a stand-alone cyber insurance policy? (Check all that apply)



Note: Respondents could choose more than one option.
*Only asked of nonbuyer respondents with cyber in standard policies.
Source: Deloitte 2019 Middle Market Cyber Insurance Survey.

package policy, where cyber is neither named nor specifically excluded. Indeed, more insurers are explicitly excluding cyber from standard coverages and creating policies specifically designed for such risks to avoid any confusion that could lead to claims disputes, leaving many buyers without stand-alone policies uninsured for the exposure.[12]

One possible concern is that one-third of nonbuyer respondents said they "had a stand-alone policy at

one time but were not satisfied with it." That was the number three obstacle raised by agent/broker respondents. Poor claims experience was often cited as a deciding factor, along with concerns about cost as well as insufficient and/or unclear coverage. The fact that many nonbuyers once had a stand-alone policy but declined to renew it indicates insurers could have significant problems to address not only to generate new sales, but to keep existing clients satisfied.

Are agents/brokers on board?

Another potentially problematic finding was the tepid support for stand-alone coverage among many agents and brokers. More than 20 percent of nonbuyer respondents said they didn't have stand-alone either because their agent or broker had not suggested it—or worse, they had advised against purchasing it.

Only one-half of those without coverage said their agent had even approached them about stand-alone insurance without being asked, versus two-thirds of those who had bought a stand-alone policy. Meanwhile, respondents who have stand-alone are more likely than those without any cyber coverage to be satisfied with their agents' knowledge of cyber risk and assessment of their cyber insurance needs.

This raises a fundamental challenge for many insurers offering stand-alone—convincing their own distribution force to enthusiastically market the product and training them to be able to do so more effectively. Part of the problem could be the additional time and effort agents and brokers often need to devote to stand-alone sales. One way this could be addressed would be to offer agents and brokers higher commission incentives for sales to first-time buyers.

What might insurers learn from stand-alone buyers?

DESPITE THE NUMEROUS concerns and objections cited by those taking a pass on stand-alone cyber coverage, and the apparent lack of support by some agents and brokers in marketing the policies, many middle market buyers have taken the plunge. Their experiences and opinions about stand-alone provide actionable insights into what insurers may need to do to increase market penetration.

Among those only with stand-alone, 41 percent of respondents bought the coverage mostly based on the results of an independent company's cybersecurity assessment. This indicates a recommendation by an objective cyber expert would likely carry more weight than advice from an insurer or intermediary, which may be regarded as a de facto sales pitch.

However, the survey also found that fear was perhaps the biggest factor driving the purchase decision (figure 7). Respondents often bought stand-alone policies as a reaction to cyberattacks against others—competitors, supply chain participants, and even companies outside their own industries.

Not surprisingly, having first-hand experience with a cyberattack seemed to make a big difference in the purchasing behavior of those surveyed. About one-third of all buyer respondents cited an attack against their company as a motivator to get cyber insurance. Indeed, 74 percent of those with both stand-alone and coverage in standard policies had a cyber-related loss in the prior three years, while only 36 percent of those without any cyber coverage said they had been hit.

This suggests those who have already been breached should be prime prospects for cyber insurance, while those who have not will likely be a much harder sell. These "uninitiated" buyers may need to be convinced about their vulnerability and the implications of not having cyber insurance after an event—most likely by documenting the experience of other policyholders in their industry.

Experience of the actual purchaser counts

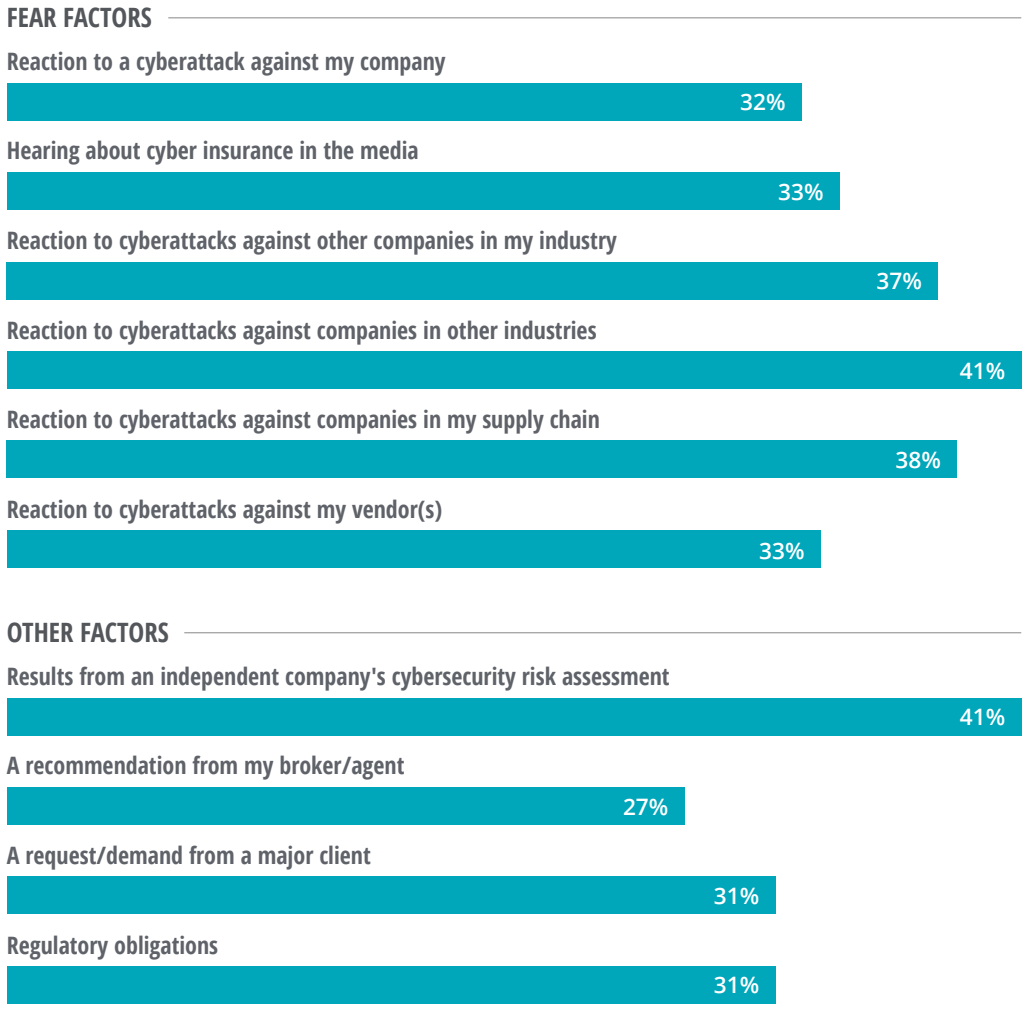
Another interesting finding was that the more experienced the buyer, the more likely they were to get a stand-alone policy. Seventy-one percent of respondents who had purchased insurance for their companies for more than 10 years had the coverage. But among buyers with one to three years of experience, only 47 percent bought cyber coverage, falling to 36 percent for those in their first year on the job. This indicates that experienced buyers may not only be more aware of cyber risks and the need to get additional, dedicated coverage, but also may be in a more credible position to persuade their C-suite about its importance.

Insurers should therefore be arming their distribution force with the latest statistics to highlight the likelihood and potential fallout of a cyberattack for those unfamiliar with the risk or the insurance available to cover it. They also should use real-life examples as case studies to clearly demonstrate not only how a stand-alone policy might help mitigate the damage of an attack,

FIGURE 7

Fear often motivates the purchase of stand-alone cyber insurance

Reasons companies bought a stand-alone cyber insurance policy



Source: Deloitte 2019 Middle Market Cyber Insurance Survey.

but why, in many circumstances, coverage in a standard policy alone may not get the job done.

The stage could already be set for such a conversation. Of those surveyed without any cyber coverage, only 51 percent said they had sufficient resources to cover losses and expenses from a cyberattack, compared with 64 percent of those with cyber in their standard policies and 71 percent of those with only stand-alone policies. Among those without any coverage, just 40 percent said they are well-prepared to prevent the vast majority of cyberattacks, while only 47 percent felt they are well-prepared to limit the damage. That's compared to about 60 percent on both counts among respondents with stand-alone and/or standard coverage.

Many agents are not actively selling stand-alone

Since cyber insurance is not yet a standard, let alone mandatory coverage, carriers will likely depend heavily on their distribution force to get the word out and help convince clients about the need for stand-alone policies. Yet it appears many agents and brokers are not enthusiastically marketing the coverage. That was certainly the case among agents of many of the nonbuyers surveyed, as noted earlier.

However, even among buyers, the respondent's agent or broker was rarely the first to suggest the purchase of a stand-alone policy. Only 6 percent of these respondents said their agent was the lead catalyst. Higher-level C-suite officials, especially the buyer's CEO, were often the first to prompt discussion over whether to buy stand-alone.

Still, a distributor's opinion can make a big difference once the subject is broached. Twenty-seven percent of respondents who already had cyber in their standard policies said their agent/broker's recommendation was the top reason they ultimately bought stand-alone coverage.

While intermediaries may dominate middle market transactions, insurance companies bypassed them and reached out directly to nearly 20 percent of respondents who had only stand-alone coverage, talking up the need for a dedicated policy. Particularly for insurers looking to restrict or exclude cyber in standard policies, this finding reveals that more proactive direct marketing could make a big impact, paving the way for greater stand-alone sales.

MOST BUYER RESPONDENTS ARE SATISFIED WITH STAND-ALONE POLICIES

The good news for insurers is most stand-alone buyers surveyed indicated they are happy with their premium and coverage, and those who filed claims had a mostly positive experience. Among all stand-alone buyers surveyed, 60 percent had filed claims and only about 9 percent of that segment were dissatisfied.

However, 36 percent of respondents who only had a stand-alone policy and filed claims were less than fully satisfied, including 25 percent who were dissatisfied. This could be troublesome. Remember that among nonbuyer respondents who had a stand-alone policy but didn't renew, many cited claims dissatisfaction as a key reason for dropping the coverage.

How could cyber insurers expand middle market penetration?

EVEN THOUGH NONBUYERS cited a host of reasons why they didn't have a stand-alone policy, 56 percent of those surveyed without any cyber coverage said they were likely to buy one in the next two years, along with 61 percent of those who already have coverage in standard policies.

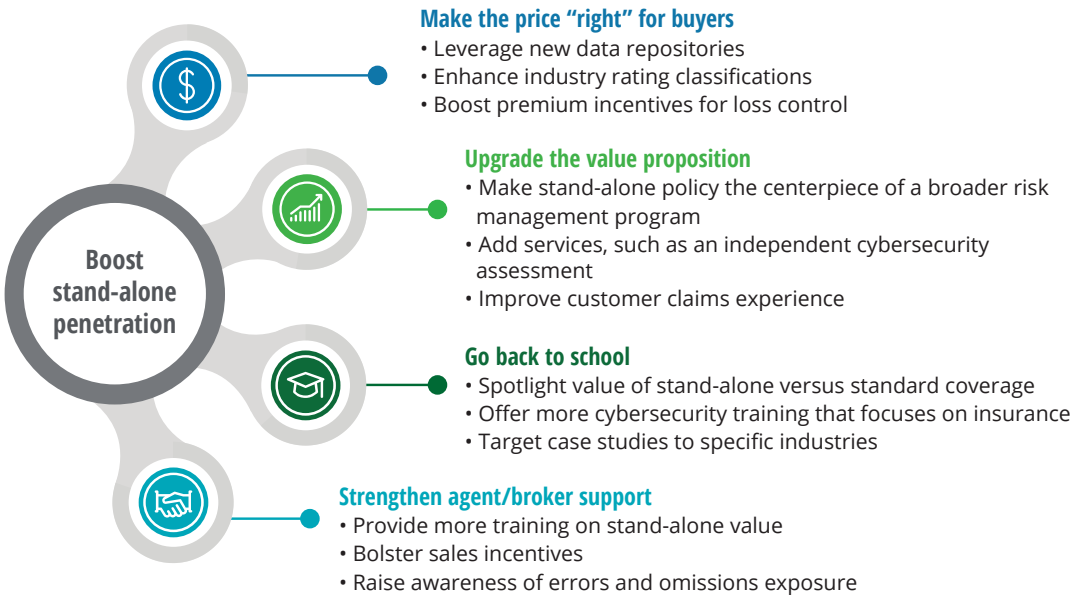
So, how can insurers convert skeptical prospects into stand-alone policyholders (figure 8)? To create greater demand for stand-alone policies, here are a few options to consider:

Rethink pricing strategies

Nonbuyers surveyed said if they did buy stand-alone, their number one motivator would be lower prices. A recent cyber insurance report by the Insurance Information Institute and J.D. Power reiterated this point, concluding that insurers, agents, and brokers "might be able to increase their overall support of this market by addressing the issues of affordability and coverage limitations that seem to be an obstacle to purchasing."[13]

FIGURE 8

Techniques cyber insurers could use to raise stand-alone penetration



Source: Deloitte Center for Financial Services analysis.

The question is how to address an issue as fundamental yet problematic as pricing. At Advisen's 2019 Cyber Risk Insights Conference last October, speakers from various cyber underwriters and brokers indicated that technical rates (based on actuarially sound analysis and probabilistic models) are still generally the exception rather than the rule. As a result, many carriers may be relying on market rates, driven by what the competition is charging. Indeed, according to a report by AIR, which models catastrophe risks, "Cyber underwriting and pricing today tend to be more art than science, relying on many subjective measures to differentiate risk."[14]

Even so, while insurers should be able to stratify pricing by industry and type of business, reliable technical pricing may remain elusive, given the evolving nature of cyber risk. This also could render historical data somewhat irrelevant as new threat actors and attack techniques continue to emerge. Insurers also should be wary of aggregation risks, where a single cyber event could potentially trigger multiple losses under different policies or impact many customers simultaneously and result in a cyber catastrophe.[15]

Given such volatility, can insurers afford to spur more stand-alone cyber policy sales by simply lowering prices or offering more coverage for the same premium, and then hoping for the best? Some margin for error may yet remain. A report by A.M. Best noted that the loss ratio for paid claims and defense costs and containment on stand-alone remains low, at only 23.2 cents out of every insurance premium dollar in 2018, mainly because of the relatively lower number of claims for cyber overall thus far, and pricing strategies that often have "carriers apply higher loads owing to uncertainty, compared to other lines."[16] By comparison, the property and casualty industry's overall loss ratio was 60.7 in 2018, which jumps to 70.4 when loss adjustment expenses are included.[17] (One caveat: Best noted that "these cyber insurance numbers could change when 2019 results are compiled, as insurers are witnessing challenges in managing increasing ransomware claims."[18])

But if carriers decide to narrow their margins to lower prices and make coverage more attractive, might they risk paying a steep price down the road? Consider the potential long-term impact of evolving exposures yet to be fully factored into the pricing equation, including ransomware, regulatory fines for data and privacy breaches, and private action settlements.

Upgrade the value proposition by adding services, incentives

Alternatively, rather than ease price resistance by cutting rates, insurers could add value by including stand-alone coverage as part of a comprehensive cybersecurity program. Thirty-one percent of nonbuyer respondents without any cyber coverage cited this as a factor that could convince them to buy a stand-alone policy. The addition of service offerings to stand-alone was ranked as the third most persuasive development that could lead to a sale, topped only by a lower price and being hit by a cyberattack. Twenty-four percent of those with cyber coverage included in standard policies also cited this factor.

In addition, a 2018 Deloitte survey examining how middle market insurers and their intermediaries could differentiate themselves by offering a broader range of products and services found buyers were particularly interested in cybersecurity support to prevent or contain attacks.[19] In addition, about 60 percent of agents and brokers surveyed for this cyber insurance report are already offering complementary cybersecurity services. Among the services agent/broker respondents said they can arrange are cyber incident response, crisis management, and forensics support, as well as loss control advice and training.

A prime purchase motivator for stand-alone buyers surveyed was "results from an independent cybersecurity risk assessment," a factor cited by 41 percent of respondents. Insurers and their intermediaries could start a stand-alone pitch by arranging a cyber assessment by an independent third party, with ongoing risk management services offered as part of a stand-alone purchase. Fifty-five percent of agents/brokers surveyed said they can "routinely provide cybersecurity assessments by qualified specialists."

Taking lessons from usage-based insurance in the personal auto segment, insurers could offer premium incentives on stand-alone coverage for those agreeing to a cyber risk assessment, ongoing monitoring services, and implementation of recommended cybersecurity measures. "As the market matures, discount incentives could serve as a motivation to purchase a cyber policy as well as increasing an organization's cybersecurity posture on the front-end," noted a report by the Council of Insurance Agents and Brokers.[20]

This could help agents and brokers market the coverage by offering a more effective, wider-ranging suite of cyber services, beyond just the annual sale of another insurance policy. It would also help plug a potential coverage gap and address a major emerging risk before competing intermediaries use cyber services beyond insurance as leverage to quote an entire commercial account.

Some carriers, brokers, and professional services providers are already working together to deliver cybersecurity support beyond risk transfer, just as they often do with other specialty lines. For example, Marsh is partnering with an array of insurers to help clients pick effective cybersecurity products and services,[21] while CNA Hardy has launched a series of partnerships to offer cybersecurity legal support and crisis management.[22]

In any case, to accelerate the market's growth, carriers will likely need to move away from the idea that cyber insurance is just about price and coverage terms. Instead, they could concentrate on making a stand-alone policy part of a holistic risk management services package that feels more valuable to customers overall.

Educate buyers and brokers

Ignorance is not bliss when it comes to cybersecurity. Indeed, as a report from the Insurance Information Institute and J.D. Power noted: "Changing company owners' perception that they don't need coverage may require a longer-term education strategy and coordination between agents and brokers and their insurers."[23]

Take the challenge of selling prospects on the need for stand-alone when they already have some cyber coverage in standard policies. One financial services chief risk officer (CRO) surveyed wrote that before they would consider buying stand-alone, their broker must "convince us that our current [standard] coverage is inadequate," while a health care CRO said their broker did not "explain to me why it would cover something not already covered." A broker surveyed wrote, "I would like for clients to be able to better understand what stand-alone policies have to offer that may, in the long run, be better for their bottom line as well as their business."

Insurers, therefore, should more aggressively plant the seeds for stand-alone cyber policy sales if they expect to accelerate market growth. Our survey shows that less experienced insurance buyers and those at companies lucky enough to have been spared a serious cyberattack will likely require the most education to warn them about the risks they face and how stand-alone insurance can better help mitigate losses. Many prospects are likely open to

such outreach efforts—30 percent of survey respondents who don't have any cyber coverage said they would be likely to buy stand-alone if they received "more education on the benefits of owning a cyber policy."

One key lesson would be for insurers and their intermediaries to point out to buyers that they cannot take it for granted their standard policies will provide adequate (or any) cyber coverage.

Over the last few years, many insurers have tried to clarify whether standard policies even cover cyber, following claims disputes over "silent" coverage (when cyber isn't explicitly named in a policy, but isn't specifically excluded either). Buyers attending a Risk and Insurance Management Society conference were warned about potential "trapdoors" and "landmines" in standard policies that could leave a company exposed if their risk manager and broker did not negotiate with carriers to affirmatively cover cyber risks and establish clear terms and limits.[24]

Such discussions should open the door to allow for a fuller explanation of the benefits of stand-alone, as either a supplement or alternative to including the risk in a standard policy. Some cyber carriers have already taken the hint about the need to raise awareness by bolstering educational efforts. For example, in 2018, Hiscox launched an online cybersecurity training platform for clients, the CyberClear Academy, which has engaged with more than 2,500 companies.[25]

Beyond educating prospects, agent/broker training is also likely essential to substantially grow the market. Insurers should demonstrate to their intermediaries how stand-alone cyber policies can close coverage gaps in a client's insurance portfolio, and therefore should be purchased as routinely as are other common specialty lines, such as D&O or EPLI.

On the flip side of this argument, intermediaries also should be made aware of the potential professional liability exposure they could face if an uninsured or underinsured client is hit with a cyberattack. Consider what happened after Superstorm Sandy, when many businesses sued their agents for failing to recommend separate flood or business interruption policies to supplement their standard property coverage.[26]

Alternative coverage options could threaten cyber insurers

IN HINDSIGHT, EARLY expectations of exponential growth in stand-alone cyber insurance may have been overly bullish. However, that doesn't mean the market is not worth pursuing. The exposure's growing prominence; the fact that more insurers are restricting, if not excluding, cyber from standard policies; and the line's relatively low loss ratio all seem to indicate strong growth potential.

Insurers appear to have room to experiment on prices, limits, and coverage terms, as well as marketing approaches. Still, carriers may not have a lot of time to adapt because they are not operating in a vacuum. As insurers contemplate shifts in strategy to increase stand-alone adoption, they should not take their place in the cyber insurance market for granted. Companies looking to alleviate cyber risk have other options.

Self-insurance is one alternative. Coverage options checked as acceptable possibilities by current nonbuyers surveyed range from setting aside a dedicated cyber risk reserve fund (cited by 51 percent) to creating their own captive insurer (42 percent), to securitizing the risk by floating cyber bonds in the capital markets (41 percent). The latter example would follow the lead of buyers who sought greater certainty and control over their property coverage in potential disaster zones via the sale of catastrophe bonds.

Additional competition may come from entrepreneurial InsurTechs. Some have already entered the market—both competing with and supporting legacy carriers. For example, startup At-Bay (formerly known as CyberJack) is working with the Hartford Steam Boiler Inspection and Insurance Company to provide both cyber risk management and stand-alone coverage.[27]

Overall, the lesson here is that if the industry doesn't come up with more attractive insurance solutions for a risk as prevalent and important as cyber, other options will likely fill the void. If that happens, insurers would be denied arguably the biggest organic growth opportunity in an otherwise mature property and casualty market. Eventually, this coverage gap could also hamstring carriers looking to maintain the rest of their standard book of business with clients and brokers.

How big might the cyber insurance market eventually be? To better manage expectations, it might help to establish a more achievable benchmark. While going from US$2 billion in premiums to US$20 billion over the next few years may not be realistic, the steps we outline here could help insurers accelerate growth well beyond the 8-to-12 percent figures of the past two years.

Over the course of the decade, sales could potentially reach D&O insurance levels—a line whose growth was also spurred, in part, by rising frequency and the threat of class-action suits. D&O direct written US premiums hit US$6.6 billion in 2018.[28] For cyber insurers, reaching even this level would represent more than a tripling of current cyber premiums and a six-fold rise in stand-alone coverage.

Despite insurers' struggles, cyber remains a promising growth opportunity. Indeed, A.M. Best "expects the current profitability of cyber insurance to attract more competition," particularly "as cyber insurance moves from being a luxury to a necessity." This can occur, according to the rating agency, "as businesses become more cognizant of the risks involved," which means that eventually, cyber insurance may yet turn out to be "an essential part of an insurer's portfolio of offerings."[29]

Endnotes

1. Hiscox, *Cyber readiness report*, 2019.
2. Ibid.
3. Ibid.
4. Allianz Global Corporate & Specialty, *A guide to cyber risk: Managing the impact of increasing connectivity*, September 2015.
5. S&P Global Market Intelligence data.
6. A.M. Best, *Best market segment report: Cyber insurers are profitable today, but wary of tomorrow's risks*, June 17, 2019. Copyright A.M. Best, used with permission.
7. Aon Cyber, *US cyber market update: 2018 US cyber insurance profits and performance*, June 2019.
8. Hiscox, *Cyber readiness report*.
9. Marsh, *2019 global cyber risk perception survey report*, 2019.
10. Hiscox, *Cyber readiness report*.
11. Marsh, *Global insurance market index—2019 Q3*, November 12, 2019.
12. A.M. Best, *Best market segment report: Cyber insurers are profitable today, but wary of tomorrow's risks*. Copyright A.M. Best, used with permission.
13. Insurance Information Institute and JD Power, *Smaller doesn't mean safer: While small companies recognize the growing cyber threat, many remain reluctant to insure against it*, October 25, 2019.
14. AIR, *Insuring cyber risk: What is holding cyber insurance back, and how can the industry push forward?*, 2017.
15. Swiss Re Institute, *Cyber: getting to grips with a complex risk*, 2017.
16. A.M. Best, *Best market segment report: Cyber insurers are profitable today, but wary of tomorrow's risks*. Copyright A.M. Best, used with permission.
17. S&P Global Market Intelligence data.
18. A.M. Best, *Best market segment report: Cyber insurers are profitable today, but wary of tomorrow's risks*. Copyright A.M. Best, used with permission.
19. Sam Friedman, Michelle Canaan, and Nikhil Gokhale, *Building new ecosystems in middle market insurance*, Deloitte Insights, February 12, 2018.
20. Council of Insurance Agents and Brokers, "Cyber insurance discount incentives," accessed November 20, 2019.
21. Andrew G. Simpson, "Marsh partners with insurers on program to help firms pick best cybersecurity products," *Insurance Journal*, March 27, 2019.
22. Charlie Wood, "CNA Hardy bolsters cyber offering with new pre-breach partnership," Reinsurance News, May 20, 2019.
23. Insurance Information Institute and JD Power, *Smaller doesn't mean safer: While small companies recognize the growing cyber threat, many remain reluctant to insure against it*.

24. Sam Friedman, "Policy 'landmines' keeping cyber insurance buyers up at night," National Underwriter, May 29, 2017.

25. Hiscox, *Cyber readiness report*.

26. Andrea Wells, "E&O dangers for agents," *Insurance Journal*, November 4, 2013.

27. Elana Ashanti Jefferson, "InsurTech startup At-Bay pairs cyber insurance with risk management," National Underwriter, December 5, 2017.

28. Carrier Management, "U.S. D&O premiums inch higher in 2018: A.M. Best," May 31, 2019.

29. A.M. Best, *Best market segment report: Cyber insurers are profitable today, but wary of tomorrow's risks*. Copyright A.M. Best, used with permission.

Acknowledgments

The author, **Sam Friedman**, wishes to thank the following Deloitte research project team members for their support and contribution to this report: **Jim Eckenrode**, **Val Srinivas**, **Prachi Ashani**, **Michelle Canaan**, and **Nikhil Gokhale**. The author also wishes to thank **Stefano Buschi** and **Ruben Frieiro** for their insights and contributions to the report.

About the author

Julie Bernard | juliebernard@deloitte.com

Julie Bernard is a principal with Deloitte Risk and Financial Advisory and is the insurance sector leader for Cyber Risk Services at Deloitte & Touche LLP. She has more than 20 years of experience serving the world's top financial institutions at the intersection between business process and information technology. With an extensive background in security strategy, privacy, consumer authentication, fraud prevention, and threat management, she helps clients be more secure, vigilant, and resilient in the face of an ever-increasing array of cyber threats and technology complexity. She is a past board member of the Executive Women's Forum and currently sits on the Advisory Board for the Financial Services Information Sharing and Analysis Center (FS-ISAC). She earned her BA in music and business administration at Westminster College and an MBA in finance at Rensselaer Polytechnic Institute.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Practice leadership

Julie Bernard
Partner | Deloitte Risk and Financial Advisory | Cyber Risk Services | Deloitte & Touche LLP
+ 1 704 227 7851 | juliebernard@deloitte.com

Daniel Soo
Principal | Deloitte Risk and Financial Advisory | Cyber Risk Services | Deloitte & Touche LLP
+ 1 212 436 5588 | dsoo@deloitte.com

Mark Nicholson
Principal | Deloitte Risk and Financial Advisory | Cyber Risk Services | Deloitte & Touche LLP
+ 1 201 499 0586 | manicholson@deloitte.com

The Deloitte Center for Financial Services

Jim Eckenrode
Managing director | The Deloitte Center for Financial Services | Deloitte Services LP
+ 1 617 585 4877 | jeckenrode@deloitte.com

Sam Friedman
Senior manager | Deloitte Services LP | Insurance research leader
Deloitte Center for Financial Services
+ 1 212 436 5521 | samfriedman@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors
Editorial: Karen Edelman, Blythe Hurley, Rupesh Bhat, and Anya George Tharakan
Creative: Sonya Vasilieff and Rajesh Venkataraju
Promotion: Hannah Rapp
Cover artwork: Sonya Vasilieff

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

About Deloitte